NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

New ND oil rules would ban most open waste pits. North Dakota oil regulators are planning new rules on the state's fracking industry, the Associated Press reported September 20. The rules include a ban on most open waste pits at oil well sites. The rules would also encourage oil companies to disclose the chemicals they use in "fracking" oil wells. North Dakota's Department of Mineral Resources director said the oil industry needs a "lighter environmental footprint" in the state. The director is expecting oil companies will be drilling thousands of wells in western North Dakota in the coming years. North Dakota Petroleum Council president said oil companies will be reviewing the proposals. Source: http://www.valleynewslive.com/story/15507194/new-nd-oil-rules-would-ban-most-open-waste-pits

Regional

(Minnesota) **Pagami Creek firefighting force tops 830 people.** More than 830 people were helping stamp out the remnants of the Pagami Creek fire September 22 in the Superior National Forest in Minnesota. Crews have more than 30 percent of the fire contained thanks to help from several aircraft, bulldozers, firetrucks, and more. But more than an inch of rain since September 18 has been the biggest factor, along with cool weather. Fire officials September 21 once again redefined the fire's boundary and downgraded the total acres to 93,669 acres, down from the original estimate of 100,000 acres. About 9,274 acres outside the Boundary Waters Canoe Area Wilderness (BWCAW) was burned over by the fire. Most of the BWCAW is now open to the public, except for entry points and routes that lead into the fire area. Nearly all roads are open, except for small forest and county roads north of Minnesota Highway 1 and Lake County Highway 7. The fire started August 18 with a lightning strike and grew into a major fire September 11 and 12. Source: http://www.duluthnewstribune.com/event/article/id/210000/

National

Scientists test early earthquake warning systems. Six months after the massive earthquake and tsunami in Japan, scientists in the United States have started testing out a new warning system to alert Americans before a big quake. The experiments are under way in California, ground zero of seismic activity in the United States, and though it might only provide a few seconds' warning, scientists say even that can make a big difference and save lives. The National Research Council presented a 20-year road map to preparing the country for earthquakes, including quietly testing new warning systems. One early test involves a map of the state lighting up on a computer screen, with a red dot signifying an earthquake's point of origin. A clock then appears signaling a countdown to impact at key locations miles away from the starting point. The system only saves seconds at this point, and is not yet broadcast to residents or businesses. With more testing, scientists hope to create an early warning system similar to one in Japan that sends text messages and interrupts television programs when

sensors detect a quake. It cost the Japanese $500 million to create, but is credited with saving lives during the 9.1-magnitude earthquake that caused a devastating tsunami. Source: http://abcnews.go.com/Technology/scientists-test-early-earthquake-warnings/story?id=14566075

INTERNATIONAL

Libyan rebels discover Gaddafi's chemical weapons. Libyan rebel forces claim to have discovered banned chemical weapons stockpiles in southern desert areas captured in the last few days from loyalists to Libya's deposed leader. Spokesmen for the National Transitional Council (NTC) said a depot had been found in Jufra, 435 miles south of Tripoli. CNN reported from Sebha that the tribe of the former Libya leader was ready to surrender its weapons and negotiate an agreement. Libya was supposed to have destroyed its entire stockpile of chemical weapons in early 2004 as part of a rapprochement with the West. It also abandoned a rudimentary nuclear program. But the international watchdog, the Organization for the Prohibition of Chemical Weapons, had stated it believed Libya had kept 9.5 tons of mustard gas at a secret location: it is that which appears to have now been captured and secured. In 2010, Libya destroyed nearly 15 tons of sulphur mustard, which is about half of its stockpile. It received an extension to eliminate the rest by May 15. Twice-yearly inspections have found no evidence of Libya reviving the chemical weapons program. Source: http://www.guardian.co.uk/world/2011/sep/22/libyan-rebels-gaddafis-chemical-weapons?newsfeed=true

Radioactive sea pollution from Fukushima may dwarf previous estimates. The Asahi Shimbun reported September 10 that more than 15 quadrillion becquerels of radioactivity may have been released from Japan's crippled Fukushima No. 1 nuclear power plant into the sea between March 21 and April 30, according to a preliminary analysis by the Japan Atomic Energy Agency (JAEA) and other institutions. That is more than three times the initial estimate of marine contamination by the plant's operator, Tokyo Electric Power Co., which said only 4.72 quadrillion becquerels had been leaked. The assistant principal researcher of coastal engineering at the JAEA said his team used the actual measurements of seaborne radioactivity near the nuclear plant's water outlets to estimate the amount of direct discharge of radioactivity. They also conducted simulations to quantify the amount of radioactive fallout from the air and added the two results together. They concluded 11.4 quadrillion becquerels of iodine-131 and 3.6 quadrillion becquerels of cesium-137 leaked into the sea. With the inclusion of cesium-134, which was not estimated, the researchers said the total amount of radioactivity was likely to exceed 15 quadrillion becquerels. Source: http://www.asahi.com/english/TKY201109090241.html

BANKING AND FINANCE INDUSTRY

Malware distribution campaign uses legal threats. Security researchers warn that an e-mail-based malware distribution campaign is threatening users with lawsuits to trick them into opening malicious attachments. In an attempt to gain credibility, the rogue e-mails purport to

originate from the Investment Company Institute (ICI), the national association of U.S. investment companies. The spam bear various subjects, most of them threatening in nature, such as, "We are going to sue you", "FW: This is a final warning", "We've sent you a copy of a complaint" or "A message from our security service". The spammers actually accuse targeted users of sending spam. The messages reads, "Your email is sending spam messages! If you don't stop sending spam, we will be impelled to sue you!" The purpose of the threat is to convince users to open the attached file, which the spammers claim is a document detailing the problem. The attachment contains a trojan downloader. "When the trojan triggers, it copies itself to the system path under the Startup folder and deletes itself," Websense security researchers warned. "Whenever you start the computer, the trojan will execute. This trojan can connect to remote servers and download malicious files." Source: http://www.theinquirer.net/inquirer/news/2110905/malware-distribution-campaign-legal-threats

E-mail addresses and passwords stolen after BitCoin forum hack. A flaw in the Bitcointalk forum was taken advantage of by a hacker and used to gain access to passwords, e-mail addresses, and personal messages belonging to members, Softpedia reported September 12. The BitCoin Web site was also hacked earlier in 2011 and private information was leaked as a result. The Web site was hit more than a week ago, during which time the attacker could freely roam and steal anything. Bitcointalk administrators only realized the site was compromised after the hacker began adding JavaScript codes. The hacker launched a SQL injection to exploit a vulnerability where the forum software did not correctly handle the escape characters found in username details. The password hashing process was made by using the Secure Hashing Algorithm (SHA-1), which experts recently discovered as being more ineffective than initially presumed. The attacker managed to hijack the account of one of the administrators, after he made a donor account that allowed him to change usernames. With the use of administrator privileges, he was able to inject PHP code by making modifications to one of the forum's style templates. Bitcointalk representatives claim the accounts overtaken or created in the process were identified, along with a series of IP addresses. Source: http://news.softpedia.com/news/Email-Addresses-and-Passwords-Stolen-After-BitCoin-Forum-Hack-221187.shtml

Chemical and Hazardous Materials Sector

Nuclear plant information among targets in Mitsubishi cyberattack. At least eight viruses infected servers at Mitsubishi Heavy Industries (MHI) in Japan, the company acknowledged September 20, with nuclear plant data believed to be among the targets of a coordinated cyberattack. MHI is a leading defense contractor in Japan, and also provides a wide range of products and design services to the civilian nuclear industry. The viruses infected 45 servers and 38 individual computers, and also put data on weapons systems at risk. International media quoted Japanese government officials as saying they are not aware of any sensitive information being accessed during the attack. Nonetheless, the government demanded that MHI conduct an investigation, which the company said will be complete by the end of September. The attack occurred in August, MHI reported. It originated outside the company's computer network and

may have revealed some MHI information, such as IP addresses. Source: http://nuclearstreet.com/nuclear_power_industry_news/b/nuclear_power_news/archive/2011/09/21/nuclear-plant-information-among-targets-in-mitsubishi-cyberattack-092102.aspx

(Nevada) **Nuclear Regulation Commission allows Yucca closure to continue.** A divided Nuclear Regulatory Commission (NRC) September 10 allowed the U.S. President to continue with plans to close the Yucca Mountain, Nevada, nuclear waste repository. The commission split, 2-2, on whether to uphold or reject a decision by an independent nuclear licensing board. The board voted in 2010 to block the Department of Energy from withdrawing its application for Yucca Mountain. The licensing board said the government failed to make a scientific case for why the application should be withdrawn. Despite the split vote, the NRC said in an order September 10 that the licensing board should continue steps to close out work on Yucca Mountain by the end of September, citing "budgetary limitations." Source: http://www.tri-cityherald.com/2011/09/10/1634806/nrc-allows-yucca-closure-to-continue.html

Commercial Facilities

(Washington) **Feds: Wi-fi hacking burglars targeted dozens of Seattle-area businesses.** A federal grand jury has indicted three Seattle men accused of hacking the wireless networks of more than a dozen businesses to steal money and employees' personal information, the Seattle Post Intelligencer reported September 19. Also claiming the trio was behind 41 burglaries, prosecutors contend the men used the fruits of their network break-ins to further the crime spree, which allegedly ran from April 2008 to at least until 2 of the men were arrested in December 2010. Prosecutors claim the men "used a variety of methods to gain unauthorized access to the computer networks of small and medium-sized businesses located in the Puget Sound region." Among those methods was "wardriving," in which hackers mount a high-strength wi-fi receiver inside a car and search for networks that can be penetrated. Once a wi-fi network is located through wardriving, hackers can remotely watch for data that may reveal the network's security setup and vulnerabilities. From April 2008 until December 2010, they stole data from at least 13 Seattle-area businesses while also burglarizing at least 41 businesses in the same region, according to the indictment unsealed September 19. Source: http://www.seattlepi.com/local/article/Feds-Wi-Fi-hacking-burglars-targeted-dozens-of-2178421.php#page-1

Communications Sector

Anonymous supporters claim NBC News Twitter hack. Hackers calling themselves the Script Kiddies took control of the NBC News Twitter account September 9, and used it to send out a series of hoax Twitter messages claiming there was a repeat terrorist attack on New York City's Ground Zero. The Script Kiddies had control of the account, which has more than 120,000 followers, for 10 minutes before it was suspended. During that time, they sent three messages stating hijackers had crashed two airplanes on the site of the September 11th attacks. That s_kiddies Twitter account was immediately suspended, but according to a cached version of the page, the group describes themselves as "Anonymous Supporters :: Hackers :: Exploiting

simplistic methods with hilarious results :: Occasionally doing it for teh lulz :: We are The Script Kiddies." Script kiddies is a hacking term, referring to technically unsophisticated hackers who rely on automated scripts to conduct online attacks. Source: http://www.computerworld.com/s/article/9219909/Anonymous_supporters_claim_NBC_News_Twitter_hack

CRITICAL MANUFACTURING

NHTSA recall notice - Daimler trucks fuel line leaks. The National Highway Traffic Safety Administration announced September 23 that Daimler Trucks North America is recalling 73,500 model year 2004 through 2008 Freightliner, Sterling, and Western Star model heavy trucks manufactured from July 11, 2003 through September 28, 2007 equipped with EPA04 model MBE4000 engines built with plastic low-pressure fuel lines and fuel filters mounted near the center of the engine on the left-hand side. The plastic low pressure fuel line between the engine mounted fuel filter and engine block may develop a substantial diesel fuel leak. This could create a road hazard increasing the risk of a crash. Fuel leakage, in the presence of an ignition source, could result in a fire. Daimler Trucks will notify owners and the remedy will be performed by Detroit Diesel Corporation authorized repair facilities. Vehicles will be inspected and the plastic low-pressure fuel line will be replaced with a steel low-pressure fuel line. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=11V478000&summary=true&prod_id=205702&PrintVersion=YES

NHTSA recall notice - Subaru Legacy and Outback. The National Highway Traffic Safety Administration announced September 12 that Subaru is recalling 195,080 model year 2010-2011 Outback and Legacy vehicles manufactured from January 7, 2010, through May 20, 2011. Components inside the wiper motor bottom cover may overheat. If the bottom cover overheats, the windshield wipers may become inoperable, reducing the operator's visibility, which may increase the likelihood of a crash or a fire. Subaru will notify owners, and dealers will replace the front wiper motor bottom cover assembly. The safety recall is expected to begin November 2011. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=11V469000&summary=true&prod_id=695826&PrintVersion=YES

NHTSA recall notice - Saab 9-2X, Subaru Forester and Impreza. The National Highway Traffic Safety Administration announced September 12 that Subaru is recalling 295,123 model year 2002-2007 Impreza, model year 2003-2008 Forester, and model year 2005-2006 Saab 9-2X vehicles manufactured from September 5, 2000 through November 26, 2007 originally sold, or currently registered in, Massachusetts, Maryland, Michigan, New Hampshire, Pennsylvania, New York, Vermont, Wisconsin, Connecticut, Delaware, Iowa, Illinois, Indiana, Maine, Minnesota, Missouri, New Jersey, Ohio, Rhode Island, West Virginia, and Washington, D.C. The front lower control arms may break at the hanger brackets due to corrosion if the hanger bracket is exposed to salty and humid environments such as roads containing snow melting agent. A broken control arm can result in the loss of control of the vehicle, increasing the risk of

a crash. Subaru dealers will inspect the degree of corrosion of the front lower control arms, and will either rustproof or replace them. The safety recall is expected to begin November 2011. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=11V464000&summary=true&prod_id=204373&PrintVersion=YES

Nearly 311,000 Honda Pilot SUVs recalled for front seat belts. The U.S. National Highway Traffic Safety Administration (NHTSA) and American Honda issued a recall of nearly 311,000 2009-2011 model year Honda Pilot SUVs for concerns over the sport utility vehicles' front seat belts, Consumer Reports reported September 12. Both the NHTSA and Honda report the stitching that holds the driver's and front passenger's seat belt to their respective anchor webbings may be missing or incomplete. Such flaws may allow the seat belt to detach from its anchor during a collision and increase the risk of injury. Honda said it will begin to notify affected owners on or near October 3, and advise them to bring their Pilots in to local dealerships. Technicians there will inspect the front seat belts and, if necessary, will perform the repair for free. Source: http://news.consumerreports.org/safety/2011/09/nearly-311000-honda-pilot-suvs-recalled-for-front-seat-belts.html

Defense/ Industry Base Sector

U.S. expresses concern over cyberattacks in Japan. The United States gave a stern warning September 21 over recent cyberattacks on Japan's top defense contractors, the latest in a series of security breaches that have fueled worries over Tokyo's ability to handle delicate information. An online assault on defense contractors including Mitsubishi Heavy Industries (MHI), which builds F-15 fighter jets and other American-designed weapons for Japan's Self-Defense Forces, began in August but came to light only earlier the week of September 19, prompting rebukes from Japanese officials over the timing of the disclosure. IHI Corp., a military contractor that supplies engine parts for fighter jets, may have also been a target, the Nikkei business daily reported. MHI said September 19 its computer systems were hacked and some network information may have been compromised. According to the company, 83 computers and servers at 11 locations, including its Tokyo headquarters, factories, and a research and development center were accessed in the attack. Details of the breach were still unclear, a company spokesman said September 21. Japan's defense minister said he did not receive reports that any classified information was compromised. It also remained unclear where the attacks originated, he said. However, an investigation by a security company revealed connections were made to 14 overseas sites, including at least 20 servers in China, Hong Kong, the United States, and India, according to the Yomiuri Shimbun, Japan's largest daily. MHI has built F-15 fighter jet and missile systems, including Patriot batteries, and AIM-7 Sparrow air-to-air missiles, designed in the United States. The company builds some of that equipment with American contractors, including Raytheon and Lockheed Martin. Source: http://www.nytimes.com/2011/09/22/world/asia/us-expresses-concern-over-cyberattacks-in-japan.html?_r=1

Schwartz: F-22 grounding ends this week. The F-22 Raptor will take to the air September 21 after 4 months on the ground for safety reasons. The U.S. Air Force Chief of Staff announced an end to the fleetwide stand-down September 19 — first in a letter to Congress, then in a statement posted on the Air Force's Web site. The chief approved a plan developed by Air Combat Command that allows the 160 twin-engine fighters to fly above 50,000 feet — the Raptor flies at 60,000 feet in normal circumstances — after an extensive inspection of every aircraft's life support systems. The systems also will be inspected daily. In addition, the plan calls for pilots to undergo physiological tests and to use additional protective equipment, although the statement did not specify the equipment. In his statement, the Chief said he based his decision on studies conducted by the Air Force Scientific Advisory Board, which has been investigating the Raptor since the stand-down took effect May 3. Source: http://www.defensenews.com/story.php?i=7725181&c=AME&s=AIR

Emergency Services

Report highlights benefits and drawbacks of social media during disasters. When it comes to disaster response, social media has proven to be a popular and effective tool for sharing information — except when the information is incorrect or malicious, in which case it hinders response efforts. That conundrum is one of the drawbacks that limit the usefulness of social media in emergency situations, according to a new report from the Congressional Research Service, which was released publicly September 13 by the Federation of American Scientists. Networks such as Facebook and Twitter have been used for sharing warnings and disaster information, contacting friends during a crisis and raise funds for disaster relief. Government agencies use such tools primarily for pushing information to the public, such as links to hurricane forecasts and evacuation routes. Some emergency management agencies are using social tools to help gather and share data in real-time, such as locations of trapped survivors. However, using social media in such situations has risks, the service warned. “While there may be some potential advantages to using social media for emergencies and disasters, there may also be some potential policy issues and drawbacks associated with its use,” the report said. For example, studies show outdated, inaccurate or false information has been disseminated via social media forums during disasters, the report said. In some cases, the location of the hazard or threat was inaccurately reported, or, in the case of the Japanese tsunami, some requests for help were retweeted repeatedly even after victims were rescued. Another concern is some individuals or organizations might intentionally provide inaccurate information to ”confuse, disrupt, or otherwise thwart response efforts,” the report said. This could be for a prank or as part of a terrorist act. Source: http://fcw.com/articles/2011/09/16/social-media-for-disasters-has-good-and-bad-aspects-crs-report-says.aspx

Energy

(California; Arizona) **Investigation: massive outage took 11 minutes.** An investigation by the California Independent System Operator (ISO) revealed there was not enough coordination between the five power system operators impacted by the September 8 outage, which left several million people without power in Orange, San Diego, and Imperial Counties in California,

as well as part of Mexico and Arizona. "There were 23 major events that occurred within an 11-minute time period within five different power grids," an ISO spokeswoman said. The outage began September 8 at 3:27 p.m. when a worker in Arizona accidentally shorted the Southwest Powerlink, which feeds power to Imperial and San Diego Counties. To compensate for the loss, Imperial County started pulling power from the north, which shut down a line when it overloaded. Then, automated systems began pulling power from the San Diego area. At the same time, a power plant in Mexicali shut down and forced Baja, Mexico, to pull power from the San Diego area as well. Since San Diego was losing power to the east, it started pulling power from Orange County lines. When those lines overloaded, they shut down too. A San Diego State University professor said there should have been a barrier in place to prevent Imperial County from tapping into San Diego's power. There was no barrier or if there was, it was not working, so the entire area went black. The entire sequence of events took less than 11 minutes. The ISO spokeswoman said there are five different power operators that were impacted by the power outage. She admitted the cooperation and communication between the five needs to be improved. Source: http://www.10news.com/news/29261019/detail.html

(California; Arizona) **Utility officials seek to unravel why safeguards failed in blackout.** The failure of a single piece of equipment in Yuma, Arizona, ignited a massive blackout that left more than 4 million people without power, baffling utility officials and highlighting the vulnerability of the U.S. electrical grid. Authorities in Arizona said September 9 safeguards built into the system should have prevented the breakdown at a Yuma substation from cascading across southern Arizona and into California, and northern Mexico. Energy experts and utility officials agreed the breakdown was troubling. Among other concerns, some experts said the failure of safeguards suggest the potential for a saboteur to take down a regional power system. Arizona Public Safety (APS) officials launched an investigation to determine the precise chain of events that began early September 8 at the North Gila substation. Utility employees noticed a problem with a series capacitor, a piece of equipment about the size of a small car that helps the utility manage voltage. APS personnel were dispatched to take it offline. The largest recent single outage occurred in 2003, when virtually the entire Northeastern United States was blacked out, and 50 million people were affected. A federal investigation identified a wide range of causes, and recommended a series of improvements intended to preclude another such failure. Source: http://www.bellinghamherald.com/2011/09/09/2177468/utility-officials-seek-to-unravel.html

Food and Agriculture

New tool helps farmers prepare for natural disasters. A team of extension professionals from across the United States developed an educational tool to assist farm and ranch managers become better prepared for any disaster. The tool is called ReadyAG: Disaster and Defense Preparedness for Production Agriculture. Before disaster strikes, ReadyAG can help farmers and ranchers plan and prepare to prevent, mitigate, respond to, and recover from all types of damaging incidents. ReadyAG is designed to help identify vulnerabilities and prioritize actions to make agricultural operations more resilient and sustainable in the face of adversity. ReadyAG begins with a general preparedness assessment then has commodity-specific sections including

cattle, crops, dairy, fruit and vegetable, swine, and poultry. The assessments can be filled out online and will automatically populate a customized action plan to address items identified as high priority vulnerabilities. Source: http://southeastfarmpress.com/management/new-tool-helps-farmers-prepare-natural-disasters

(New York) **New York firm recalls chicken, beef, veal and pork products due to an undeclared allergen.** M & P Food Production Ltd., a Brooklyn, New York establishment, recalled about 11,000 pounds of chicken, beef, veal, and pork dumpling products because they may contain an undeclared allergen, milk, the U.S. Department of Agriculture's Food Safety (USDA) and Inspection Service (FSIS) announced September 20. The milk is a sub-ingredient contained in sour cream used to make the dough. Each chicken product package bears the establishment number "P-18832," and each meat product package bears the establishment number "EST 18832" inside the USDA mark of inspection. The products were produced between March 18 and September 19, and distributed to retail establishments in Connecticut, Florida, Massachusetts, North Carolina, New Jersey, New York, Ohio, Pennsylvania, and South Carolina. The problem was discovered by an FSIS inspector while conducting a label review. The inspector noticed the use of sour cream in making dough for the products, but no indication of milk as an ingredient on the label. The FSIS and the company have received no reports of adverse reactions due to consumption of these products. Source: http://www.foodconsumer.org/newsite/Shopping/Alerts/recalls_chicken_beef_veal_and_pork_products_0920111103.html

(Wisconsin; Illinois; Minnesota) **Roundy's recalls chicken sold in Ill., Minn., Wis.** Roundy's Supermarkets Inc. based in Milwaukee, Wisconsin, recalled about 360 pounds of breaded chicken breast that may have been undercooked. The U.S. Department of Agriculture (USDA) said the products were sold after September 13 at deli counters in Illinois, Minnesota, and Wisconsin. The agency said the product being recalled was no longer available for purchase, but consumers who already bought it should discard it. The product is called "Chef's Collection Chicken Milanese Breast." The container has the identifying item code of "037496," and lot code of "171589-2561." The USDA said the problem was discovered after a consumer complaint. It said Roundy's thinks one tray of chicken did not undergo the final cooking process. No illnesses have been reported. Source: http://www.cnbc.com/id/44625203

Study finds dangerous chemical in kids' canned goods. Many canned foods have a potentially cancerous chemical called Bisphenol A, or BPA, in the plastic lining of the can, according to a new study by the Breast Cancer Fund (BCF). Released September 21, the report found the toxin in six canned foods marketed to kids. "BPA in laboratory studies has been linked to increased risks for breast cancer, prostate cancer, early puberty," BCF's policy manager said. The study found large amounts of BPA ranging from 13 parts per billion (ppb) to 114 ppb in everything from canned soup to pasta and spaghetti products. BPA is used in the plastic lining of the cans, and expeets have said it leaches from the plastic into the food. Many cancer researchers believe BPA in children is of particular concern because it may set the stage for disease later in life. But chemical firms and Campbell Soup Co., a manufacturer of many of the food products reviewed in the study, have said the levels of BPA in canned foods are too low to be harmful.

The BCF said companies should switch to can liners that are free of BPA. In the meantime, the organization suggests parents use alternatives to canned food, such as dried or frozen pasta or soups packaged in Tetra Paks, made mostly from paper. Source: http://www.wishtv.com/dpp/health/study-finds-dangerous-chemical-in-kids-canned-goods

(Montana) **Equine Infectious Anemia confirmed in Carbon County mule.** A 32-year-old mule in Carbon County, Montana, was diagnosed with equine infectious anemia (EIA), Montana Department of Livestock reported September 20. Also known as swamp fever, EIA is a potentially fatal viral disease of equines spread by biting insects. No vaccine or treatment is available for the disease. The infected mule was discovered when a Coggins test –- a screening test required for equine movement into or out of the state –- was performed for out-of-state movement. The test was positive, and was confirmed by the federal National Veterinary Service Laboratories (NVSL) in Ames, Iowa. Follow-up testing on two other equines at the premises, which is currently under quarantine, is underway. The premises is in a remote area with limited potential for exposure to other equines. Due to strict regulations, owners of EIA-infected equines have few options. Those options include a lifetime quarantine with a minimum of 200 yards distance between the quarantined animal and other equines, euthanasia, and donating the animal for EIA-related research. Source: http://www.theprairiestar.com/news/equine/equine-infectious-anemia-confirmed-in-carbon-county-mule/article_cb43a726-e399-11e0-85f5-001cc4c002e0.html

(Colorado) **Cantaloupe deaths: Several dead from eating tainted cantaloupe linked to Colorado.** Four people have died in an outbreak of listeria traced to Colorado cantaloupes, the U.S. Centers for Disease Control and Prevention (CDC) said September 19. One death occurred in Colorado, one in Oklahoma, and two in New Mexico. The death count could soon rise to six. A spokesman for the New Mexico Department of Heath said the CDC is in the process of confirming two additional deaths linked to the outbreak in his state. The CDC said 35 people in 10 states have been sickened in the outbreak so far. The illnesses are in California, Colorado, Illinois, Indiana, Montana, Nebraska, New Mexico, Oklahoma, Texas, and West Virginia. Colorado has the most illnesses with 12 sickened, followed by Oklahoma with six, and New Mexico with five. The illnesses have been traced to fruit from Jensen Farms in Holly, Colorado. The Food and Drug Administration said September 19 it had found listeria in samples of Jensen Farms' cantaloupe taken from a Denver-area store, and on samples taken from equipment and cantaloupe at the farm's packing facility. Tests confirmed the samples matched the strain of the disease found in those sickened. Jensen Farms recalled its Rocky Ford-brand cantaloupes the week of September 12 after the illnesses were linked to its fruit. Source: http://www.huffingtonpost.com/2011/09/19/cantaloupe-deaths-colorado_n_970856.html

Washington creamery recalls raw milk over E.coli contamination. Pride & Joy Creamery LLC, based in Granger, Washington, has recalled raw milk because of possible contamination with Escherichia coli bacteria that can cause serious illness, RTTNews reported September 20. The recalled unpasteurized milk containers show expiration dates of September 30 and September 31, and the milk was sold at retail stores in King, Pierce, Snohomish, and Skagit counties as well as at the on-farm store in Granger, Yakima County. The recall comes after routine sampling by

the Washington State Department of Agriculture revealed the product was contaminated with toxin-producing E. coli. Investigations are ongoing to determine the source of contamination, and public health officials are examining if there is any evidence to link human illness to the contaminated milk. Source: http://www.rttnews.com/Content/BiotechStory.aspx?Id=1716961&Category=FDARecall

Government Sector (including Schools and Universities)

White powder scare causes courthouse evacuation. The Hampden County Hall of Justice was evacuated briefly September 21 after a worker opened an envelope containing a mysterious white powder in Springfield, Massachusetts. Officials said a secretary in the district attorney's office on the third floor opened the envelope around 10:45 a.m., and came into contact with the powder. They said the woman then complained that her hands were burning after she washed them. She is said to be OK. The hazardous materials team responded, and everyone was allowed back inside shortly after. "This is the kind of thing that's not going to affect the whole building or anything or affect more than that one particular room for the amount, less than a gram was there. So, I do not think there was any concern about it getting into the ventilation system or anything," said a Springfield Fire Department spokesman. The area where the powder was found remained closed. At this point it is not clear what the powder is or where the letter originated from. Source: http://www.cbs3springfield.com/story/15509748/white-powder-scare-causes-courthouse-evacuation?hpt=us_bn4

Air Force One flight plan leaked in Japan. A Japanese air traffic controller posted the U.S. President's flight plan on his personal blog, and now he could be charged for leaking national secrets. According to Daily Yomiuri Online, the President is planning a trip to Asia in November to take part at the Asia-Pacific Economic Cooperation forum meeting, and the leaked document shows detailed data about the flight from Seoul, South Korea, to Japan. The owner of the blog posted 12 images with information about Air Force One and another American drone used for surveillance work. "I wanted to show the photos to my friends and acquaintances." The land, infrastructure, transport, and tourism Ministry is the one handling the case. Its representative stated that the images, and those of three radar screens showing aircraft routes were deleted from the blog. Aviation regulations state it is forbidden to take pictures inside radar rooms and airport control rooms, but some experts claim the rules should be made stricter. A senior defense ministry official said "The movements of Air Force One have never been made public, even in the United States." Because of the air traffic controller, who is in his fifties and has been working at Haneda Airport since October 1981, Japan will be added to the list of countries that easily leaks information. Source: http://news.softpedia.com/news/AirForce-One-Flight-Plan-Leaked-221310.shtml

Information Technology and Telecommunications

Facebook attacks get automated, says Imperva. Cybercriminals have started using complex scripting techniques to automate their attacks on the Facebook social networking platform. According to Imperva researchers, with the advent of social networking, hackers have turned to sites such as Facebook to create another attack channel. However, the attacks seen to date have been typically manual, such as uploading malware or creating fake pictures. But now, according to Imperva, social engineering may be entering the next phase: automation. Recently, a new tool emerged that automates social engineering on Facebook. Unlike hacking software, this tool does not demonstrate any new theoretical security vulnerability, but its existence proves the case that automated attacks on Web 2.0 services are a real threat. Source: http://www.infosecurity-us.com/view/20862/facebook-attacks-get-automated-says-imperva/

Bluetooth vulnerabilities becoming easier to exploit. Codenomicon warns consumers about the poor quality and security of Bluetooth equipment. Based on Codenomicon's robustness test results using smart model based fuzzing tools, 80 percent of tests against various Bluetooth devices find critical issues. Every device failed with at least one test suite against a critical communication profile. Bluetooth is particularly vulnerable against malformed input. Such input may cause Bluetooth device operation to slow down or to show unusual behavior or crash. In a worst case scenario, malformed input can be used by an outside attacker to gain unauthorized access to the Bluetooth. When vulnerabilities are in low-level communication profiles such as L2CAP, they are not protected by the pairing process. These flaws can be exploited without the user accepting or even noticing the connection. So far, Bluetooth quality and security has not been perceived as a problem. The pairing process and conformance testing is thought to provide enough protection. Bluetooth applications have not offered access to confidential data so there has been little motivation to attack the Bluetooth interface. However, Bluetooth is becoming more and more critical. Modern car kits and healthcare equipment, for example, use Bluetooth technology. Source: http://www.net-security.org/secworld.php?id=11663

50,000 Web sites infected with spam from 'Wplinksforwork'. A large WordPress poisoning was discovered after the infection-spreading Web site was shut down and error messages began appearing on the compromised pages. A Google search returned 53,000 links that belong to locations that contain the error message. The error message revealed itself in place of some malicious links that were supposed to show up in the exploited HTML documents at the bottom of the page. After the location was taken out of service, error alerts appeared instead of the illegal ads. Besides the "wplinksforwork" domain, there is another malevolent address called "hemoviestube," which appears to be not functional at the moment. Source: http://news.softpedia.com/news/50-000-Websites-Infected-with-Spam-From-Wplinksforwork-223004.shtml

Android bug lets attackers install malware without warning. It has been more than a month since researchers reported two serious security vulnerabilities in Android, but so far there is no indication when they will be purged from the Google operating system that is the world's most popular smartphone platform. The first flaw allows apps to be installed without prompting

users for permission. This permits attackers to surreptitiously install malware in much the way a proof-of-concept exploit a researcher published in 2010 did. In that case, an app he planted in the Android Market and disguised as an expansion pack for the Angry Birds game secretly installed three additional apps that without warning monitored a phone's contacts, location information, and text messages so data could transmitted to a remote server. The second bug resides in the Linux kernel where Android originates and makes it possible for installed apps with limited privileges to gain full control over the device. The vulnerability is contained in code the device manufacturer has put into some of Android's most popular handsets, including the Nexus S. The bug undermines the security model Google developers created to contain the damage any one application can do to the overall phone. Source: http://www.theregister.co.uk/2011/09/20/google_android_vulnerability_patching/

Cisco warns of vulnerability in its Identity Services Engine. Cisco is warning users of a critical vulnerability (CVE-2011-3290) in its Identity Services Engine (ISE). In its security advisory, the company said the underlying database used by ISE, its identity and access control policy platform, contains three sets of default credentials that could be exploited by a remote attacker without any end-user interaction. Using these credentials, an attacker could modify the configuration and settings, or even gain complete administrative control of adevice. All hardware appliance and software-only versions of Cisco ISE prior to 1.0.4.MR2 are affected. The company said it will release a free update to the software to address the vulnerability September 30; no temporary workaround is available. Once released, the updates will be available to download from the Cisco Software Center. Source: http://www.h-online.com/security/news/item/Cisco-warns-of-vulnerability-in-its-Identity-Services-Engine-1347301.html

New DroidDream variant has ability to fight off other malware. DroidDream, a malicious program that targets Android devices, received a major overhaul, and now contains more features for stealing data and phishing the owners of compromised Android phones and tablets, according to a Trend Micro researcher. The latest update to the DroidDream malware, which Trend labeled "ANDROIDOS_DORDRAE.N" is spreading over third party mobile application Web sites, mostly in China. Building on earlier versions of the DroidDream malware, it includes expanded data theft capabilities, allowing remote attackers to siphon off SMS messages, call logs, mobile contact lists, and information related to Google accounts that may be stored on the compromised Android device, according to Trend's research blog. Source: http://threatpost.com/en_us/blogs/new-droiddream-variant-has-ability-fight-other-malware-091911

Crooks push fake anti-virus via Skype calls. Scareware pushers have turned to Skype with automated messages to pressure users into buying worthless security software. The scam is promoted via unsolicited calls on Skype during which a machine-generated message warns potential victims their computer security is "out-of-date." Victims are invited to visit a Web site selling fake anti-virus software for $19.95. The robotic message states: "Attention: this is an automated computer system alert. Your computer protection service is not active. To activate computer protection, and repair your computer, go to..." Users are confronted with the

alarming alert when they click on a message from an account called "URGENT NOTICE." Source: http://www.theregister.co.uk/2011/09/20/skype_scareware_scam/

National Monuments and Icons

(Texas) **Texas fire destroys 1,554 homes, 17 people missing.** The number of homes destroyed by a Texas wildfire has risen to 1,554 and is expected to further increase as firefighters enter more areas where the fire has been extinguished, officials said September 11. At least 17 people remain unaccounted for. Bastrop County officials joined by a U.S. Representative sought to provide new information to hundreds of residents evacuated from their homes a week ago when blustering wind whipped up by Tropical Storm Lee swept across parched, drought-stricken Texas, helping to spark more than 190 wildfires statewide. The worst of the fires has consumed more than 34,000 acres in an area 30 miles southeast of Austin. Officials said at a news conference September 11 that people would begin going back into the scorched areas September 12. A detailed plan will allow residents to slowly enter the evacuated areas over the coming week as firefighters and emergency responders ensure the land has properly cooled, hotspots are extinguished, and the fire is contained. Source: http://www.timesunion.com/news/article/Texas-fire-destroys-1-554-homes-17-people-missing-2165776.php

Postal and Shipping

Nothing Significant to Report

Public Health

Hospital drug shortages deadly, costly. An Associated Press review of industry reports and interviews with nearly two dozen experts found at least 15 deaths in the past 15 months blamed on drug shortages, either because the right drug was not available or because of dosing errors or other problems in administering or preparing alternative medications. A hearing on the issue was set for September 23 before the health subcommittee of the House Energy and Commerce Committee. The Food and Drug Administration is holding a meeting September 26 with medical and consumer groups, researchers, and industry representatives to discuss the shortages and strategies to fight them. Just over half of the 549 U.S. hospitals responding to a survey this summer by the Institute for Safe Medication Practices, a patient safety group, said they had purchased one or more prescription drugs from so-called "gray market vendors" — companies other than their normal wholesalers. These vendors buy scarce drugs from small regional wholesalers, pharmacies or other sources and then market them to hospitals, often at many times the normal price. These sellers may not be licensed, authorized distributors. Source: http://www.forbes.com/feeds/ap/2011/09/23/health-specialized-consumer-services-us-hospitals-drug-shortages_8696656.html

Scores sick from bedbug chemicals. A report released by the U.S. Centers for Disease Control and Prevention (CDC) September 22 found that dozens of Americans have fallen ill from the insecticides used to kill bedbugs. One North Carolina woman died after using 18 cans of chemical. The report counted 80 illnesses and one death linked to the insecticides over 3 years. Most of the cases were in New York City, the apparent epicenter of a recent U.S. bedbug comeback. The CDC was able to get data from 12 states, and only seven had reports of such illnesses. In the CDC study, researchers reviewed reports from California, Florida, Michigan, North Carolina, New York, Texas, and Washington. They counted 111 cases from 2003 through 2010. Most occurred in the last few years, and more than half were in New York City. Because many of the cases, including the lone death, were do-it-yourselfers who misused the chemicals or applied the wrong product, federal health officials are warning consumers to be careful. In recent national surveys of exterminators, bedbugs were named the toughest pest to eliminate. Source: http://www.azcentral.com/news/articles/2011/09/23/20110923bedbug-chemicals-scores-sick.html

Some acid reflux drugs linked to C. diff. The popular class of acid reflux medication that includes Aciphex, Dexilant, Nexium, Prevacid, Prilosec, and Protonix is associated with an increased risk of diarrhea caused by the bug Clostridium difficile (C. diff). Japanese researchers followed about 500 hospitalized patients, over half of whom were taking these drugs, called proton pump inhibitors (PPIs). Those who were taking PPIs were more than three times as likely to develop C. diff diarrhea as those who were not taking them. but the risk of any individual patient developing the infection was relatively low, said a researcher from Teiko University in Tokyo. Overall, 19 of 487 PPI users developed C. diff diarrhea, compared with 4 of 329 people who did not take the acid-lowering drugs. The findings were reported at the Interscience Conference on Antimicrobial Agents and Chemotherapy. Source: http://www.webmd.com/heartburn-gerd/news/20110921/some-acid-reflux-drugs-linked-to-c-diff

Transportation

U.S. military satellite to get attack-warning equipment. A U.S. military satellite is to be fitted with equipment which will enable it to detect hostile action and inform ground controllers what is going on, according to reports. An Air Force general said September 21 that a classified satellite is now planned to go into space equipped with a Self-Awareness Space Situational Awareness (SASSA) package. SASSA would let a satellite know if it was being jammed, blinded, or scrambled, while other dedicated spacecraft would be able to watch events in Earth orbit and detect or monitor anti-satellite operations involving actual intercepts and collisions. Source: http://www.theregister.co.uk/2011/09/22/sassa_to_fly/

Water and Dams

(California) **South Gate properties have carcinogenic chemical in groundwater.** Federal environmental officials said they are investigating whether pollution at two Los Angeles County, California properties warrants cleanup of hazardous waste. The Environmental Protection

Agency (EPA) said it's proposing the sites in South Gate for the national priorities list under Superfund law. A metal cleaning solvent was found in soil and water testing at Seam Master Industries, and the Jervis B. Webb company. Seam Master is a carpeting company, but it is suspected the toxic contamination came from a previous tenant, a company that made screw products. Jervis B. Webb sits where a rivet manufacturer once fabricated parts in the boom days of aerospace. Shallow groundwater at both sites contains more than the maximum limit for a chemical called trichloroethylene (TCE). Studies have found TCE causes cancer when people encounter it in water. EPA officials said drinking water in deeper underground reservoirs is not yet contaminated, but they noted shallow and deeper aquifers can connect and spread pollution. The EPA plans to do a more thorough investigation of the pollution and its source. The results of that study will determine whether the properties are designated as Superfund sites. Source: http://www.scpr.org/news/2011/09/19/28930/south-gate-properties-have-carcinogenic-chemical-g/

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168